AD-A100 021 RAND CORP SANTA MONICA CA F/G 5/11
THE POTENTIAL CRIMINAL ADVERSARIES OF NUCLEAR PROGRAMS: A PORTR--ETC(U)
JUL 80 B M JENKINS
UNCLASSIFIED RAND/P-6513 NL

END
DATE FILMED
7-81
DTIC

THE POTENTIAL CRIMINAL ADVERSARIES OF NUCLEAR PROGRAMS: A PORTRAIT

Brian M. Jenkins

July 1980

14 RAND/P-6513

PREFACE

The following paper is the text of a speech presented at the 21st Annual Meeting of the Institute of Nuclear Materials Management held at Palm Beach, Florida, June 30-July 2, 1980. The speech summarizes research done under contract to Sandia Laboratories. It addresses the motivations, intentions, capabilities, and resources of potential criminal adversaries of U.S. nuclear programs.

For a detailed discussion of this work see the following Rand reports: *Attributes of Potential Criminal Adversaries of U.S. Nuclear Programs,* Peter deLeon, Brian Jenkins, Konrad Kellen, Joseph Krofcheck, R-2225-SL, February 1978; *Motivations and Possible Actions of Potential Criminal Adversaries of U.S. Nuclear Programs,* Gail Bass, Brian Jenkins, Konrad Kellen, Joseph Krofcheck, Geraldine Petty, Robert Reinstedt, David Ronfeldt, R-2554-SL, February 1980; *Terrorists--What Are they Like? How Some Terrorists Describe Their World and Actions,* Konrad Kellen, N-1300-SL, November 1979, and *Major Crimes as Analogues to Potential Threats to Nuclear Facilities and Programs,* R. N. Reinstedt and Judith Westbury, N-1498-SL, April 1980.

The possibility that terrorists or other kinds of criminals might attempt to seize or sabotage a nuclear facility, steal nuclear material, or carry out other criminal activities in the nuclear domain has created special problems for the security of nuclear programs. For many years now, Sandia Laboratories, at the direction of the Department of Energy, has played a leading role in developing and testing new measures of protection. In 1975, Sandia asked The Rand Corporation to assist it in analyzing the potential threat.

Our task was to describe the potential criminal adversary, or rather the spectrum of potential adversaries who conceivably might carry out malevolent criminal actions against nuclear programs and facilities.

We were concerned with both the motivations as well as the material and operational capabilities likely to be displayed by various categories of potential nuclear adversaries.

What utility does a study of the capabilities and intentions of potential adversaries have? Why do it? The designers of security systems and those in charge of setting the standards and making the rules make assumptions all the time about the intentions and capabilities of their perceived adversaries. Assumptions are made when safeguards and security standards are established. Assumptions are made when people in government or industry make budgetary allocations for security measures. Assumptions are made when a decision is reached to acquire or not to acquire certain kinds of security hardware or to hire additional guards instead. These assumptions may not always be explicit, but they are still made.

A study of the capabilities and intentions of potential criminal adversaries, although sometimes necessarily speculative and requiring an inferential leap from non-nuclear criminal activity to as yet uncommitted serious crimes in the nuclear domain, provides a basis for making such assumptions. It allows those making the assumptions to check with reality.

The principal methodological problem in conducting such research is that there have not been a great number of serious actions directed against nuclear facilities. No nuclear installations in the United States have been attacked, seized, or sabotaged in a way that caused

the release of radioactivity. No nuclear weapons have been stolen. No special nuclear materials have been diverted or taken by force from installations or while in transit. And no radioactive matter has been maliciously dispersed so that public safety was endangered. Although a certain amount of nuclear materials is unaccounted for, there is no available evidence that it was stolen or diverted to weapons use.

A number of bomb threats have been telephoned to nuclear facilities, a now common occurrence in both government and industry. A number of threats to use nuclear material have proved on investigation to be hoaxes. Minor sabotage has been carried out in a handful of cases.

Outside of the United States there have been a few incidents of more serious potential consequences. Urban guerrillas briefly seized control of a nuclear facility under construction in Argentina. Political extremists on several occasions have attempted to sabotage or have sabotaged operating reactors or reactors under construction in Europe. Most of these incidents occurred after we began our study.

Lacking an adequate sample of nuclear incidents from which we might build a profile of the adversaries, we expanded our study to include actual crimes outside of the nuclear domain that are in some way analogous to possible but uncommitted nuclear crimes.

Several hundred cases of conventional crimes were analyzed. We looked at sophisticated burglaries, major armed robberies, and industrial sabotage. We looked at "white-collar" crime. We also examined incidents involving political extremists, such as terrorist assaults and "symbolic" bombings, where a political statement and not the destruction of the target was the primary aim. We examined the perpetrators (arsonists, psychotic bombers and mass murderers) as well as the crimes for clues about their sometimes bizarre motivations and their capabilities. Gradually a group portrait emerged.

Let's start with why.

Understanding *why* certain adversaries might want to attack nuclear targets could help us anticipate *what* they might attempt to do and how. Nuclear defenders must anticipate a surprisingly wide range of threats from an equally wide array of potential adversaries.

Nuclear programs seem to have all of the adversaries faced by any industry as well as those faced by any industry that deals in a highly valuable commodity. Nuclear programs also attract some particular adversaries: opponents of nuclear energy and weapons development; political terrorists who view such programs as symbols of the political and economic system they wish to destroy, or who view the anti-nuclear movement as a potential constituency; emotionally unstable people obsessed by the almost mystical qualities of nuclear power. The fear evoked by the word "nuclear" itself in the minds of many people may provide a special attraction to certain categories of adversaries.

We grouped the motivations that might prompt potential adversaries to undertake criminal actions against U. S. nuclear programs into three broad categories: ideological, economic, and personal.

Ideological motivations are those linked to a political or philosophical system. They would include those of political terrorists, anti-nuclear extremists, and certain groups of philosophical or religious fanatics. These potential adversaries might target nuclear facilities hoping to influence government policy on nuclear energy or nuclear weapons; or as a way of coercing changes in other (non-nuclear) areas of government policy; or perhaps as a way of undermining public confidence in the government and promoting political unrest.

Economic motivations involve a desire for financial gain. Both professional and amateur criminals might view nuclear material or weapons as potentially attractive targets for schemes of theft for ransom, sale, or extortion.

Personal motivations emerge from the special situations of specific individuals. Personal reasons for committing a nuclear-related crime would range from those of the hostile employee seeking to redress a grievance against his employer to those of the psychotic individual responding to "celestial voices."

We did *not* examine in detail the potential for crimes against nuclear programs or facilities by agents of foreign governments. This does not reflect a judgment that such crimes are less likely or important than those that might potentially be committed by the domestic adversaries. In fact, some of the most intriguing cases involving

alleged thefts or diversion of nuclear material appear to have been the work of agents of a foreign government. But details of these cases are hard to come by. They remain cloaked in uncertainty and secrecy.

What sorts of crimes might these various adversaries attempt? Here again we noted a broad spectrum of possible intentions. They vary in seriousness from the adolescent prank to schemes of mass destruction.

We identified actions aimed at destroying or disabling nuclear facilities, actions aimed at acquiring nuclear material or information, and actions aimed at disrupting nuclear programs. We also recognized certain crimes that do not directly involve the security of U.S. nuclear facilities or programs but are nonetheless of concern because the response to such threats or actions could involve nuclear security officials and make special demands on security and safeguards systems. An example would be a nuclear extortion threat in which it becomes crucial to know whether any nuclear material has been taken.

The actions coincide with the motives. For example, a disgruntled employee (whose motivation we would label "personal") might want to inflict economic damage upon his employer, perhaps by temporarily disabling a plant, disrupting operations, or damaging equipment through such actions as vandalism, sabotage, and hoax bomb threats. Such actions would have less appeal to the group with economic motives, who would be more likely to turn to theft of material or to extortion schemes involving threats to personnel or facilities.

Political terrorists might attempt to penetrate nuclear facilities for the purpose of sabotage. They could threaten officials in nuclear programs or attempt to seize a facility as part of a campaign to disrupt nuclear programs. They could also make nuclear threats, and if they had somehow acquired SNM, actually attempt to fabricate and detonate a nuclear device of some type.

In fact, they have done at least some of these things. In Spain and in France, terrorist groups have sabotaged nuclear facilities. In Spain, they have also kidnapped and threatened to kill officials connected with nuclear programs.

These events supported one of our major conclusions. The presumed range of potential dangers to nuclear programs is *not* entirely

hypothetical. There have already been many low-level actions--bomb threats, low-level sabotage, nuclear hoaxes--that provide examples of most of the categories of perpetrators and motives we had thought of. Such low-level actions appear to have satisfied the aims of a wide range of perpetrators and therefore seem likely to occur again.

There is little basis for extrapolating from the low-level incidents to higher-level incidents. However, the last several years have witnessed an increase in the number and seriousness of nuclear-related incidents. Although we still have not seen acts of sabotage aimed at causing radioactive release, a number of incidents have occurred since we began our research in the mid-1970s in which adversaries demonstrated greater sophistication or greater willingness to cause casualties. Fortunately, only those adversaries driven by blind fanaticism or psychological abnormalities appear likely to attempt nuclear crimes aimed at producing *widespread* casualties. At the same time, it must be pointed out that owing to popular conceptions and misconceptions of nuclear energy, an incident of relatively harmless actual consequence conceivably could produce large-scale effects. A well-formulated hoax threat, for example, might conceivably cause widespread alarm, even panic.

Satisfied that we can depict the full range of motives and possible actions, we can turn our attention to an assessment of the adversaries' capabilities.

Let's start with the number of attackers. The question of how many they would come with was almost an obsession with security planners when we began our research. This was due to the fact that the popular perception of the threat was that of armed attackers assaulting a nuclear facility, guns blazing. The postulated number of attackers, according to engagement models, and computerized gun fights, would determine the number of defenders needed.

The question also turned into a challenge to the intelligence community. How many bad guys could get together to plan an action against nuclear programs without the authorities discovering the conspiracy beforehand?

Our answer was probably neither satisfying nor reassuring. Thieves and terrorists come with as many persons as they think they need to carry out their intended mission, and given their high rate of success-they figure right most of the time. Three to six was common, but that figure appears to have been determined more by operational requirements than by any resource limitations. If they need more people, and if the take is worth it, they assemble more. Crimes involving between 12 and 20 perpetrators have been seen, and in the cases we examined they managed to maintain secrecy.

How will they be armed? Outside of barroom brawls, few crimes have gone uncommitted for lack of a gun, least of all in America. Weapons and explosives are readily available in the United States. Large numbers of automatic weapons and even some precision-guided missiles have been stolen from military stocks and are available on the illicit market. Explosives are obtainable commercially or by theft, and the information necessary to manufacture explosives from readily purchased materials is easily available.

The adversaries will also be well equipped with tools and equipment such as power drills, cutting torches, radios, and other electronic gear. The primary constraint on their arms and equipment will be on how much they can carry and use, not on what they can acquire.

Available transport, in addition to automobiles and trucks, may include high-speed off-road vehicles, including some armored models, radio-controlled, explosive-filled cars or trucks for smashing through barriers, and helicopters for airborne assault or rapid escape. No operation as elaborate as the above list implies has been seen outside of wartime commando raids. However, all of the component parts have been seen individually in the crimes we examined.

In sum, the potential adversaries have little difficulty cbtaining the physical resources needed to assault an installation if that is their chosen mode of attack. Nor do they seem to encounter serious obstacles in recruiting gang members, or procuring weapons, explosives, or special equipment. Instead, the critical constraints upon the adversaries seem to lie in the less tangible realm of human capabilities: imagination and ingenuity, criminal skills, technical knowledge,

the willingness to risk capture or death, accurate intelligence or privileged access often provided by inside confederates, and the necessary combination of these ingredients.

High levels of criminal skills and technical sophistication were seen in many of the crimes we examined, particularly some of the burglaries. Sabotage and white-collar crimes also showed high levels of technical knowledge possessed by their perpetrators, who often were insiders. Profit-minded criminals, however, showed little taste for risk. They were careful, cautious men, concerned with turning a profit without being captured.

In contrast, terrorists have shown themselves more willing to accept battle, ready to kill, prepared to die. Typically, they come more heavily armed. But even terrorists, although they have taken on armed bodyguards in their kidnappings, have rarely assaulted well-defended targets. The prospect of being shot does appear to have some deterrent value.

Another thing adversaries appear to abhor is uncertainty about the security system. One way they solve that problem is to recruit inside accomplices. Inside assistance appears to be an extremely important ingredient in many high value crimes. Criminals were apparently able to suborn or coerce inside confederates, often members of the security force, in at least 31 percent of the high-value crimes we examined. Recruiting inside accomplices by threatening members of their families, a powerful form of leverage used in a number of cases, poses an especially difficult problem for defenders.

We found that internal conspiracies involving two or more employees, some quite large, were a lot more prevalent than we had imagined. Many such conspiracies have involved top management. These were the most successful from the standpoint of the size of the take and in avoiding discovery.

Overt assault by armed force might be the least likely mode of nuclear theft. The more likely mode will involve bribes, the collusion of insiders, the establishment of fronts, changes in inventory records and bills of lading, and other attributes characteristic of embezzlement, commodity diversions, and other white-collar crime.

Even overt theft is likely to begin not with armed assault over the fence but rather entry gained by means of deception and disguise. Diversions also figured in many of the episodes we examined.

The lack of a ready market for stolen nuclear material suggests that a buyer will be known to the perpetrators in advance, or even that the buyer will commission the crime, as in many art thefts.

The lack of a ready market also suggests that thieves may steal nuclear material in order to sell it back to the victims of their crime who will be anxious to minimize financial loss and the embarrassment of even admitting the loss of material.

Finally, although there is no established black market for stolen nuclear material as there is for stolen arms, there have been a number of incidents in which agents, operating on behalf of unnamed suppliers, have offered to sell nuclear material. Often the product turns out to be not SNM as billed but uranium ore or depleted uranium, neither dangerous nor very valuable. The cases nevertheless demonstrate the apparent willingness to engage in illicit nuclear traffic. Only the dearth of buyers, not the risks, preclude a nuclear black market.